PCT/GB99/04219

The Patent Office

INVESTOR IN PEOPLE

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

GB99/4219

09/868314

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

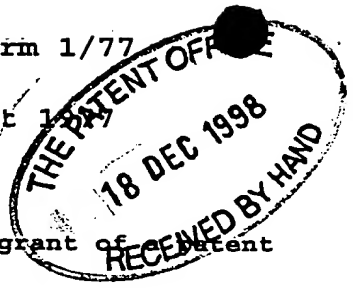
Signed M Cooke

Dated 31 January 2000

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Patents Form 1/77

Patents Act 1977
(Rule 16)



THE PATENT OFFICE

21DEC98 E413365-3 000754
P01/7700 0.00 - 9828093.6

Request for grant of a patent

The Patent Office

Cardiff Road
Newport
Gwent NP9 1RH

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

1. Your reference

23345

2. Patent application number
(The Patent Office will fill in this part)

9828093.6

18 DEC 1998

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

DAVID MICHAEL JARMAN, 11 BERKELEY STREET, MAYFAIR, LONDON W1X 6BU, UNITED KINGDOM

Patents ADP number *(if you know it)* 7572660001

If the applicant is a corporate body, give the country/state of its incorporation

4. Title of the invention

ELECTRONIC DATA STORAGE AND DISPLAY APPARATUS

5. Name of your agent *(if you have one)*

GALLAFENT & CO

"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

9 STAPLE INN
LONDON WC1V 7QH

Patents ADP number *(if you know it)*

0000729001

6. If you are declaring priority from one or more earlier patent applications give the country and the date of filing of the or of each of these earlier applications and *(if you know it) the or each application number*

Country	Priority application number *(if you know it)*	Date of filing *(day/month/year)*

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing *(day/month/year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:*

a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
(See note (d))

NO

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form	0
Description	8
Claim(s)	6
Abstract	0
Drawings	4 + 4

10. If you are also filing any of the following, state how many against each item.

Priority documents	0
Translation of priority documents	0
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	0
Request for preliminary examination and search *(Patents Form 9/77)*	1
Request for substantive examination and search *(Patents Form 10/77)*	
Any other documents *(Please specify)*	

11. I/We request the grant of a patent on the basis of this application.

Signature

Date 18 December 1998

12. Name and daytime telephone number of person to contact in the United Kingdom

GALLAFENT & CO
0171 242 3094

DUPLICATE

Electronic data storage and display apparatus

This invention relates to electronic data storage and display apparatus, and in particular to such apparatus for the storage and display of electronic data that has commercial value such as electronically formatted books.

With the advances in the fields of microchip and display screen technologies, and allied computing advances it is becoming increasingly economically viable to produce apparatus that is easily portable and can store, manipulate and display large quantities of electronic data. There is, however, often a reluctance on the part of the owners of that data to release it to members of the public because of the ease of replication of electronic data. For data with commercial value such replication deprives the parties involved with the genesis and distribution of the data of a suitable reward for the production or distribution of that data. For example, if the data when rendered legible by suitable software is the text of a book, then if the data becomes available to the public not under the control distributor, owner etc., then electronic copies of that data may easily be made and the publisher of that data will sell less copies of that book than he may otherwise sell.

The present invention provides apparatus for the transmittal, reception, storage and display of data in an electronic format in which there is provided a casing that includes a data storage means, a data display

means, and a data transmission/reception means including at least one output/input port, characterised in that the data transmission/reception means includes means for decrypting received data and placing it in the data storage means, encrypting and transmitting data from the data storage means and means for storing at least one encryption key, and in which one encryption key references addresses in a portion of Read Only Memory, and the content of those addresses is used to encrypt/decrypt transmitted/received data.

In use, for example when the user of the apparatus wishes to obtain an electronic version of a book, the user connects the apparatus of the present invention to an appropriate source of electronic data in the following manner:

i) the apparatus enters into electronic communication with the data source and sends an identification code to the data source,

ii) the data source confirms the identity of the apparatus and thereby determines what encryption key to use in communicating with the apparatus,

iii) the user of the apparatus causes the apparatus to send a code to the data source identifying the data to be received by the apparatus,

iv) the data source transmits the identified data in encrypted form to the apparatus which decrypts that

data and places it in the data storage means,

v) the data source transmits a new encryption key to the apparatus, which key overwrites the previous encryption key, and

vi) the communication between the apparatus and the data source is broken.

By having the apparatus and the data source interact in this fashion, the electronic data is encrypted when it is travelling between the owners or distributors of the data and the legitimate end user of the data. Because the encryption key between the data source and the apparatus is altered after each transaction, it will be very difficult for an illegitimate receiver of the data to decrypt that data. Even if that does prove possible, the illegitimate receiver only then gains the encryption key for one specific piece of apparatus the next time it connects to the data source and not the data source as a whole.

In a particularly preferred embodiment of the present invention the apparatus stores two encryption keys, one of which is stored in either Electronically Erasable Programable Read Only Memory or non-volatile Random Access Memory, and the other of which is stored in Read Only Memory. The encryption key in the Electronically Erasable Programable Read Only Memory or non-volatile Random Access Memory is the key that is rewritten when the apparatus interacts with a data store.

In a preferred embodiment of the present invention, the encryption key in the Electronically Erasable Programable Read Only Memory or non-volatile Random Access Memory is 16 bytes in size. The portion of Read Only Memory, the content of which is used to encrypt/decrypt transmitted/received data, is preferably 256 bytes in size.

The data storage means in the apparatus of the present invention is preferably non-volatile random access memory. It may, however, alternatively be in the form of a magnetic disk, built into the casing and so constructed that attempts to remove the disc would result in the destruction of at least the data on the disc, or any other known data storage media which could be built into the casing.

The method of communication between the apparatus of the present invention and the data store is most preferably via the telephone network, and at least one input/output port in the casing is adapted to connect to that network most preferably via an electromagnetic radiation link. In alternative embodiments other methods of connection the data source are possible and at least one input/output port in the casing is appropriately configured for that connection.

In a preferred embodiment of the present invention, the display means includes a display screen and computer hardware and software to enable presentation of the data in graphical and/or textual form. The computer hardware

preferably includes user control means which will allow a user of the apparatus to move through the data in an appropriate fashion. The display screen of the present invention is preferably of sufficient size that the viewing area thereof is at least 110mm by 180mm. The screen is preferably of a type that has a low power consumption.

In an alternative embodiment of the present invention, the apparatus additionally includes known means for the generation of sound. The sound generation means can be controlled by the computer software that controls the display means, or by independent control means. In this embodiment the reader of, for example, a book about ornithology may be played the sound of the bird which he is reading about.

It will be appreciated that the size of the data storage means in the apparatus of the present invention will be finite. As such, and to avoid the problem of either having to delete and loose a previously acquired set of data, or having to acquire a new apparatus, the apparatus of the present invention is configured so that it can export some or all of the data stored in the data storage means. To prevent duplicatable and readable copies of the data being exported, the apparatus is configured only to export the data in an encrypted form.

It is clearly desirable that the exported data can be imported back onto the apparatus of the present invention, so that the data can be viewed again at a

later date.

The data is preferably exported to and imported from a dedicated data store adapted to interact with the apparatus of the present invention. In the first preferred embodiment, the method of transfer of the data is as follows:

i) the apparatus enters into electronic communication with the data store which sends an identification code to the apparatus,

ii) the apparatus confirms the identity of the data store and thereby determines what data store encryption key to use in communicating with the data store,

iii) the user of the apparatus causes the apparatus to transfer preselected data between the apparatus and the data store in encrypted form,

iv) the receiver of the encrypted data decrypts that data and stores it,

v) the apparatus transmits a new data store encryption key to the data store, which key overwrites the previous data store encryption key, and

vi) the communication between the apparatus and the data store is broken.

In a second preferred embodiment the method of transfer of the data is as follows:

i) the apparatus enters into electronic communication with the data store,

ii) the user of the apparatus causes the apparatus to transfer preselected data between the apparatus and the data store in encrypted form,

iii) the receiver of the data stores the data, and

iv) the communication between the apparatus and the data store is broken.

In this second embodiment the data store stores the data in encrypted form. Preferably there is, however, a little un-encrypted data attached to the encrypted data. That un-encrypted data can, for example, give an indication of the contents of the data, and/or the apparatus that placed the data in the data store and consequently the apparatus that can decrypt the data. This will allow more than one piece of apparatus of the present invention to use the data store.

In either of the two above described embodiments, the data transfer between the apparatus and the data store can be either via electrical or optical cables or via electromagnetic radiation.

In one particularly preferred embodiment of the present

invention, the apparatus is provided with a computer chip that has the specification, details and method of operation as set out on attached sheets marked A1, A2, A3, and A4.

The apparatus of the present invention may be provided with it's own power source and/or means for taking power from an external power source.

Claims

1 Apparatus for the transmittal, reception, storage and display of data in an electronic format in which there is provided a casing that includes a data storage means, a data display means, and a data transmission/reception means including at least one output/input port, characterised in that the data transmission/reception means includes means for decrypting received data and placing it in the data storage means, encrypting and transmitting data from the data storage means and means for storing at least one encryption key, and in which one encryption key references addresses in a portion of Read Only Memory, and the content of those addresses is used to encrypt/decrypt transmitted/received data.

2 Apparatus according to claim 1 in which at least one encryption/decryption key is stored in a portion of either Electronically Erasable Programable Read Only Memory or non volatile Random Access Memory, and may be rewritten by an external key issuing computer.

3 Apparatus according to claim 2 in which at least one encryption key is 16 bytes in size.

4 Apparatus according to any one of claims 1 to 3 in which the Read Only Memory is at least 256 bytes in

size.

5 Apparatus according to any one of claims 1 to 4 in which the data storage means is comprised of non volatile Random Access Memory.

6 Apparatus according to any one of claims 1 to 5 in which an output/input port is adapted to connect with a telephone socket via an electromagnetic radiation link.

7 Apparatus according to any one of claims 1 to 6 in which the display means includes a display screen and computer hardware and software to enable presentation of the data in graphical and/or textual form.

8 Apparatus according to any one of claims 1 to 7 which is provided with a computer chip that has the specification, details and method of operation as set out on attached sheets marked A1, A2, A3, and A4.

9 A method of using apparatus according to any one of claims 1 to 8 for the reception of electronic data from an external data source characterised in that:

i) the apparatus enters into electronic communication with the data source and sends an identification code to the data source,

ii) the data source confirms the identity of the apparatus and thereby determines what encryption key to use in communicating with the apparatus,

iii) the user of the apparatus causes the apparatus to send a code to the data source identifying the data to be received by the apparatus,

iv) the data source transmits the identified data in encrypted form to the apparatus which decrypts that data and places it in the data storage means,

v) the data source transmits a new encryption key to the apparatus, which key overwrites the previous encryption key, and

vi) the communication between the apparatus and the data source is broken.

10 A method according to claim 9 in which the means of electronic communication between the apparatus and the data source is via the telephone network.

11 A method according to claim 9 in which the means of electronic communication between the apparatus and the data source is via the internet.

12 A method according to anyone of claims 9 to 11 in which the electronic data is electronically stored

text and/or graphics.

13 A method of using apparatus according to any one of claims 1 to 8 for the transfer of electronic data between the apparatus and an external data store characterised in that:

i) the apparatus enters into electronic communication with the data store which sends an identification code to the apparatus,

ii) the apparatus confirms the identity of the data store and thereby determines what data store encryption key to use in communicating with the data store,

iii) the user of the apparatus causes the apparatus to transfer preselected data between the apparatus and the data store in encrypted form,

iv) the receiver of the encrypted data decrypts that data and stores it,

v) the apparatus transmits a new data store encryption key to the data store, which key overwrites the previous data store encryption key, and

vi) the communication between the apparatus and the data store is broken.

14 A method of using apparatus according to any one of claims 1 to 8 for the transfer of electronic data between the apparatus and an external data store characterised in that:

i) the apparatus enters into electronic communication with the data store,

ii) the user of the apparatus causes the apparatus to transfer preselected data between the apparatus and the data store in encrypted form,

iii) the receiver of the data stores the data, and

iv) the communication between the apparatus and the data store is broken.

15 A method according to claim 14 in which the electronic data is transmitted from the data store to the apparatus, and is saved in the apparatus in decrypted form.

16 A method according to claim 14 in which the electronic data is transmitted from the apparatus to the data store, and is saved in the data store in encrypted form, the encryption key being a permanent encryption key for that data held in the apparatus.

17 A method according to any one of claims 13 to 16 in which the data store will on interrogation by the apparatus, provide the apparatus with a list of the data stored within the data store.

18 A method according to any one of claims 13 to 17 in which the means of electronic communication between the apparatus and the data store is via electrical or optical cable.

19 A method according to any one of claims 13 to 17 in which the means of electronic communication between the apparatus and the data store is via electromagnetic radiation.

20 A method according to anyone of claims 13 to 19 in which the electronic data is electronically stored text and/or graphics.

A1

SPECIFICATION

EEPROM: 16 bytes of key memory (addresses 0 - 15).
112 bytes of user memory (addresses 16 - 127).

POWER: 5mA @5V when active
6mA @5V when writing to eeprom
10uA @5V in power saving mode.

CONVERSION RATE: approx. 30KPS.

MASK LOOKUP TABLE

Rom address

0 = 255
1 = 254
2 = 253
3 = 252
4 = 251
5 = 250
. . . . . .
. . . . . .
. . . . . .
250 = 5
251 = 4
252 = 3
253 = 2
254 = 1
255 = 0

starting with address 0 = 255 the rom table is filled by the following formula :

rom table[address] = 255 - address

ENCRYPTION/DECRYPTION OPERATION

Version 1.0 of crypto uses a key length of 16 bytes.

First write the 16 byte key to eeprom addresses 0 - 15.
Each byte of key is used to access an 8 bit mask from within a 256 byte lookup table.
Each data byte is encrypted/decrypted by exclusive oring it with the 8 bit mask.
As each byte of data is encrypted/decrypted the mask is rotated one bit position to the left.
After eight bit rotations a new mask is loaded using the next key in the sequence of sixteen.
The sequence of masks will be repeated again when all sixteen have been used.

A2

OPERATION MODES

EEPROM WRITE (mode 0)

1. Wait until BUSY line is a logic low.
2. Write number 0 (binary 00000000) to PORT0.
3. Wait until BUSY line is a logic low.
4. Write eeprom address (0 - 127) to PORT1.
5. Wait until BUSY line is a logic low.
6. Write eeprom data to PORT2.

Steps 1 & 2 need only be done once to set eeprom write mode.

DECRYPT DATA (mode 1)

1. Wait until BUSY line is a logic low.
2. Write number 1 (binary 00000001) to PORT0.
3. Wait until BUSY line is a logic low.
4. Write data for decryption to PORT2.
5. Wait until BUSY line is a logic low.
6. Read decrypted data from PORT3.

Steps 1 & 2 need only be done once to set data decrypt mode.

ENCRYPT DATA (mode 2)

1. Wait until BUSY line is a logic low.
2. Write number 2 (binary 00000010) to PORT0.
3. Wait until BUSY line is a logic low.
4. Write data for encyption to PORT2.
5. Wait until BUSY line is a logic low.
6. Read encrypted data from PORT3.

Steps 1 & 2 need only be done once to set data encrypt mode.

EEPROM READ (mode 3)

1. Wait until BUSY line is a logic low.
2. Write number 3 (binary 00000011) to PORT0.
3. Wait until BUSY line is a logic low.
4. Write eeprom address (0 - 127) to PORT2.
5. Wait until BUSY line is a logic low.
6. Read eeprom data from PORT3.

Steps 1 & 2 need only be done once to set eeprom read mode.

RESET COUNTERS (mode 4)

This will reset the rotate counter & key index to zero.

1. Wait until BUSY line is a logic low.
2. Write number 4 (binary 00000100) to PORT0.

POWER SAVING (mode 5)

This will put the crypto pcb into sleep mode.

1. Wait until BUSY line is a logic low.
2. Write number 5 (binary 00000101) to PORT0.
3. Wait until BUSY line is a logic zero before proceeding.

Waking up the crypto unit from power saving mode

1. Do a dummy read from PORT0 or Write a new operation mode to PORT0.
2. Wait until BUSY line is a logic low before proceeding.